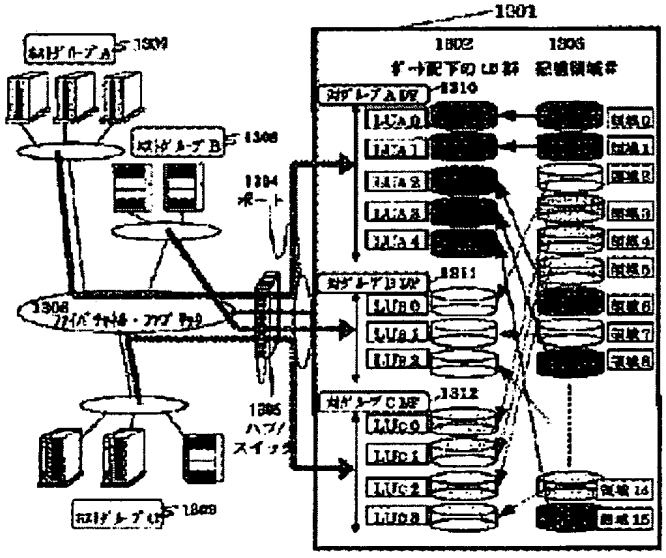
STORAGE SUBSYSTEM HAVING SECURITY FUNCTION FOR EACH LOGICAL UNIT

Patent number: JP2003030053
Publication date: 2003-01-31
Inventor: ITO RYUSUKE; OKAMI YOSHINORI; UCHIUMI KATSUHIRO; IGARASHI YOSHINORI; HORI KOICHI
Applicant: HITACHI LTD
Classification:
- International: G06F12/14; G06F3/06; G06F12/00
- european: G06F3/06M; H04L29/06C6
Application number: JP20010213642 20010713
Priority number(s): JP20010213642 20010713

Also published as:
EP1276034 (A2)
US6779083 (B2)
US2003014600 (A1)

Abstract of **JP2003030053**

PROBLEM TO BE SOLVED: To solve the problem that security by every logical unit is not realized while efficiently using system resources by the conventional LUN(logical unit number) security function in a storage subsystem to which access from various computers is expected. SOLUTION: The storage subsystem is provided with a table to regulate an a information WWN (world wide name) to uniquely identify a computer, an information GID(group ID) to identify a group to which the computer belongs and a logical unit number LUN in the storage subsystem to which access from a host computer is permitted by an operating method optional to a user and to disclose the logical unit number to a host computer. Propriety of access to the logical unit in the storage subsystem is determined by unit of group to a group of computers optionally grouped by the user by using a management table in the storage subsystem.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－30053
（P2003－30053A）
(43)公開日　平成15年１月31日(2003.1.31)

(51)Int.Cl.[7]	識別記号	ＦＩ	テーマコード（参考）
Ｇ０６Ｆ　12/14	３１０	Ｇ０６Ｆ　12/14	３１０Ｋ　５Ｂ０１７
3/06	３０１	3/06	３０１Ａ　５Ｂ０６５
12/00	５３７	12/00	５３７Ａ　５Ｂ０８２

審査請求　未請求　請求項の数９　ＯＬ　（全 17 頁）

(21)出願番号　特願2001－213642(P2001－213642)

(22)出願日　平成13年７月13日(2001.7.13)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　伊東　隆介
神奈川県小田原市中里322番地２号　株式会社日立製作所ＲＡＩＤシステム事業部内
(72)発明者　岡見　吉規
神奈川県小田原市中里322番地２号　株式会社日立製作所ＲＡＩＤシステム事業部内
(74)代理人　100075096
弁理士　作田　康夫

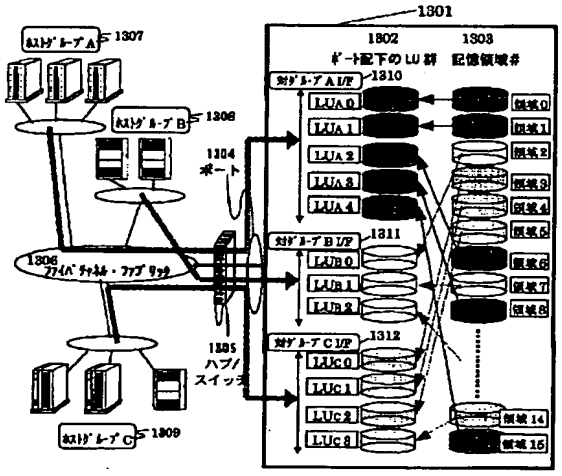
最終頁に続く

(54)【発明の名称】　論理ユニット毎のセキュリティ機能を備えた記憶サブシステム

(57)【要約】　（修正有）

【課題】　多種多様なコンピュータからのアクセスが想定される記憶サブシステムにおいて、従来のＬＵＮセキュリティ機能ではシステムの資源の有効利用を図りつつ、論理ユニット単位でのセキュリティを実現できなかった。

【解決手段】コンピュータを一意に識別する情報WWN（ＷｏｒｌｄＷｉｄｅＮａｍｅ）と、このコンピュータが属するグループを識別する情報ＧＩＤ（Ｇｒｏｕｐ ＩＤ）と、このホストコンピュータからのアクセスを許可した記憶サブシステム内の論理ユニット番号ＬＵＮを、ユーザ任意の運用方法に基づいて規定し、ホストコンピュータに対して開示するテーブルを設ける。記憶サブシステム内の管理テーブルを用いることによって、ユーザが任意にグループ化したコンピュータ群に対し、そのグループ単位で記憶サブシステム内の論理ユニットに対するアクセス可否を決定できる。



【特許請求の範囲】
【請求項１】複数のコンピュータに接続するためのインタフェースを適用可能なポートと、
前記ポートを経由して前記コンピュータからアクセス可能な論理ユニットと、
前記論理ユニットに格納すべきデータを格納する１つ又は複数の記憶装置と、
前記記憶装置に対してデータの読み書きを制御する記憶制御装置を有する記憶サブシステムにおいて、
前記論理ユニットにアクセスするコンピュータを、重複を許して、グループに分け、
各グループに１つ又は複数の論理ユニットを割り当て、
割り当てた論理ユニットと前記記憶装置の記憶領域とを、重複を許して、対応させる管理テーブルを設けたことを特徴とする記憶サブシステム。
【請求項２】請求項１記載の記憶サブシステムであって、前記管理テーブルは、更に、
前記グループ分けしたコンピュータの各グループと、前記割り当てられた論理ユニットとを対応させるインタフェース情報を有する記憶サブシステム。
【請求項３】請求項１記載の記憶サブシステムであって、更に、保守用端末装置を接続可能な通信制御部を有し、
前記通信制御部に通信回線を介して保守用端末装置を接続し、前記管理テーブルの内容を変更できる記憶サブシステム。
【請求項４】請求項１記載の記憶サブシステムにおいて、
前記割り当てた論理ユニットと前記記憶装置の記憶領域とを、重複を許して、対応させることにより、前記クループ分けされた各グループ相互の論理ユニット単位でのセキュリティを機能させることを特徴とする記憶サブシステム。
【請求項５】請求項１記載の記憶サブシステムにおいて、
前記ポートを経由してアクセスしてくるコマンドから、そのコマンドを送出したコンピュータを特定する情報を抜き出し、
その特定する情報が前記管理テーブルに存在したときは、前記グループに分けたコンピュタであるとして、前記割り当てた論理ユニットへのアクセスを許し、
その特定する情報が前記管理テーブルに存在しなかったときは、前記グループに分けたコンピュータでないとして、前記アクセス可能な論理ユニットへのアクセスを許さない機能を有する記憶サブシステム。
【請求項６】請求項５記載の記憶サブシステムにおいて、
前記機能を、コンピュータの問合せコマンド発行の際にのみ発揮させ、一度、前記割り当てた論理ユニットへのアクセスを許した後は、前記問合せに係るコンピュータからのコマンドを受け付ける記憶サブシステム。
【請求項７】請求項６記載の記憶サブシステムにおいて、
前記割り当てた論理ユニットへのアクセスを許した後は、当該論理ユニットの番号と、当該論理ユニットに対応した前記記憶装置の記憶領域の番号との対応付けには、前記問合せに係るコンピュータのグループの番号を使用する記憶サブシステム。
【請求項８】複数のコンピュータ又は記憶サブシステムに接続するためのインタフェースを適用可能なポートと、
前記ポートを経由して前記コンピュータからアクセス可能な論理ユニットと、
前記論理ユニットに格納すべきデータを格納する１つ又は複数の記憶装置と、
前記記憶装置に対してデータの読み書きを制御する記憶制御装置を有する記憶サブシステムにおいて、
前記論理ユニットにアクセスするコンピュータを、重複を許して、グループに分け、
各グループに１つ又は複数の論理ユニットを割り当て、
割り当てた論理ユニットと前記記憶装置の記憶領域とを、重複を許して、対応させる管理テーブルを、
前記ポートを介して接続された記憶サブシステムと共用することを特徴とする記憶サブシステム。
【請求項９】複数のコンピュータ、ハブ、スイッチ又はルーターに接続するためのインタフェースを適用可能なポートと、
前記ポートを経由して前記コンピュータからアクセス可能な論理ユニットと、
前記論理ユニットに格納すべきデータを格納する１つ又は複数の記憶装置と、
前記記憶装置に対してデータの読み書きを制御する記憶制御装置を有する記憶サブシステムにおいて、
前記論理ユニットにアクセスするコンピュータを、重複を許して、グループに分け、
各グループに１つ又は複数の論理ユニットを割り当て、
割り当てた論理ユニットと前記記憶装置の記憶領域とを、重複を許して、対応させる管理テーブルを、
前記ポートを介して接続されたコンピュータ、ハブ、スイッチ又はルーターと共用することを特徴とする記憶サブシステム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】コンピュータからアクセスされる記憶サブシステムに係り、特に、記憶サブシステム内の論理ユニットのアクセスに関する。
【０００２】
【従来の技術】近年、ファイバチャネル・プロトコルが規格化され、それをインフラとしてＳＡＮ（Ｓｔｏｒａｇｅ Ａｒｅａ Ｎｅｔｗｏｒｋ）環境が複雑、多様化し

てきた。この結果、記憶サブシステムにつながるコンピュータの数と種類若しくはＯＳ（Ｏｐｅｒａｔｉｏｎ Ｓｙｓｔｅｍ）の種類、並びに記憶サブシステムに要求される論理ユニット数が大幅に増加している。また記憶サブシステムとコンピュータとのインタフェースに、ファイバチャネルの他、ＳＣＳＩや、ＥＳＣＯＮ、ＴＣＰ／ＩＰ、ｉＳＣＳＩなど様々なプロトコルが同時に使用される環境が整いつつある。尚、ここで、コンピュータとは、ネットワークに接続可能な電子回路を有する電子機器をいう。

【０００３】このような環境では、多種多様のコンピュータが１つの記憶サブシステムに対してアクセスしてくることを意味する。コンピュータには、いわゆる大型のホストコンピュータや、小型の個人用のコンピュータも含まれるが、種々のコンピュータが記憶サブシステムにアクセスする場合に、適宜、「ホストからアクセスする」、「ホストコンピュータからアクセスする」等の表現を用いる。

【０００４】この状況下では従来のホスト側のＯＳやミドルウェア、アプリケーション・ソフトウェアに頼った記憶サブシステム資源に対するセキュリティ機能では不十分であると危惧されるようになり、論理ユニット（以下、適宜、ＬＵと略す）に対する不正アクセスを防止する強固なＬＵＮセキュリティ機能の必要性も急速に高まってきている。尚、ＬＵＮとは、記憶サブシステム内の論理ユニット番号をいう。

【０００５】記憶サブシステム資源（論理ユニット）に対するセキュリティ機能の実現手段として、特開２０００－２７６４０６がある。左記公報による方法では、記憶サブシステム内のＬＵＮに対するアクセス可否に関して、セキュリティ機能を実現しているものの、単一のポートに対してアクセスしてくる多種多様のコンピュータには、対応できず、実際の運用上は単一ポート配下で管理可能なホストコンピュータ種を１種類とするものである。この実際の運用上の制限は、先に述べたＳＡＮ環境の急激な拡張等の状況に追随できない。

【０００６】

【発明が解決しようとする課題】記憶サブシステム内の論理ユニットを、ＬＵＮセキュリティ機能を伴いつつコンピュータに提供すべく、記憶サブシステムの単一ポート配下に、従来よりも多数の論理ユニットを定義づけ、複数のＯＳを有するホストコンピュータ、ＯＳの種別が異なる複数のコンピュータその他コンピュータ群に開示する必要がある。

【０００７】しかし従来の記憶サブシステムのＬＵＮセキュリティ機能では、単一ポート配下で管理可能なホストコンピュータが多数あってもＯＳの種類は同一でなければならず、さらに単一ポートに設定可能なホストコンピュータとの接続上のインターフェース設定も１通りのみという制限が一般的であり、最近のＳＡＮ環境に対する課題となっていた。このような課題を解決すべく、単純に、記憶サブシステムの単一ポート配下に多数の論理ユニットを定義し、当該ポートにアクセスしてくる複数種類のＯＳに対して、そのまま分割・開示する方法が考えられる。

【０００８】しかし、現状のコンピュータの種々のＯＳは、記憶サブシステムの論理ユニットゼロ（ＬＵ０）にアクセスできない場合には、そのＬＵ０の次のＬＵ１以降の同系列のＬＵに対しては、その存在を全く問い合せない仕様となっている。因みに、ＳＣＳＩ－２の規格では、この１系列は８つのＬＵで構成されるため、ＬＵ０～ＬＵ７までが同系列となる。

【０００９】このため、記憶サブシステム内の論理ユニット番号（ＬＵＮ）をそのままホストコンピュータに開示したのでは、論理ユニット設定側の期待通りには、コンピュータに論理ユニットが正しく認識されないという課題があった。

【００１０】また、現状のコンピュータの種々のＯＳは、単一ポート配下に認識し得る論理ユニット数の上限を２５６個とするものが多く、論理ユニット数を２５７個以上設けても認識されないこととなり、この点も記憶サブシステム内の論理ユニットを単一ポート配下でコンピュータに開示する上での課題となっていた。

【００１１】一方、記憶サブシステムにおいて、強固なＬＵＮセキュリティ機能を提供する場合において、コンピュータから送信されてくるコマンドに関して、逐一、対象ＬＵに関するアクセス可否をチェックする方法が最も堅牢ではあろうが、記憶サブシステムにおける処理時間（セキュリティーチェックのためのオーバーヘッド）が大きくなってしまい性能上の課題となっていた。

【００１２】そこで、本発明の第１の目的は、コンピュータの既存の処理、制限その他の機能を変更せずに、コンピュータをＯＳその他任意の種別毎にグループ化して、そのグループ化されたコンピュータがアクセス可能な論理ユニットを制限し、そのグループ単位にインターフェース上の設定を可能とし、ＬＵＮセキュリティ機能を記憶サブシステムの単一ポート配下において提供可能とすることである。また、本発明の第２の目的は、上記セキュリティ機能を、記憶サブシステムの高速なアクセス判定ロジックと共に提供することである。

【００１３】

【課題を解決するための手段】記憶サブシステムを次の構成とする。即ち、コンピュータ（ホストコンピュータを含む）を一意に識別する情報（ＷＷＮ:Ｗｏｒｌｄ Ｗｉｄｅ Ｎａｍｅ）、このコンピュータが属するグループを識別する情報（ＧＩＤ:Ｇｒｏｕｐ ＩＤ）、このコンピュータからのアクセスを許可した記憶サブシステム内の論理ユニット番号（ＬＵＮ）の対応を記述した管理テーブルと、これを格納する不揮発のメモリと、コンピュータが記憶サブシステムにログインする際に動的に割

り当てられ、以降、ログアウトするまで有効であるユニークな管理番号（S_ＩD）、コンピュータを一意に識別する情報（WWN）、およびこのホストコンピュータが属するグループを識別する情報（ＧＩＤ）の対応を記述した管理テーブルと、これを格納する不揮発のメモリと、これら管理テーブルを設定する１つ以上の入力端末と、１つ以上の記憶装置と、これらの記憶装置に対してデータの読み書きを制御する記憶制御装置と、コンピュータと接続を行うための１つ以上のポートと、前記記憶装置の記憶領域に対応した論理ユニット（ＬUN）を有する記憶サブシステムとする。

【００１４】この記憶サブシステムにおいては、コンピュータの既存の処理、制限その他の機能を変更せずに、単一ポート配下で、ユーザが、任意のコンピュータのグループ単位に、アクセス可能なＬUN設定や接続インターフェース上の設定を行なえるため、単一ポート配下で、複数の種類のＯＳを備えたコンピュータ群を対象に、アクセスコントロール機能、すなわちＬUNセキュリティ機能を実現することができる。

【００１５】また、この記憶サブシステムにおいては、ホスト識別情報WWNの代わりに、ログインの際に割り当てるS_ＩDをもとにＧＩDを識別情報として用いるため、アクセス可能なＬUNを判定する際の時間が、WWNを用いる場合に比べて簡易であるため少なくて済み、高速である。

【００１６】

【発明の実施の形態】本発明では、記憶サブシステムとコンピュータ間で使用するインタフェース・プロトコルの例としてファイバチャネルを用い、その上で動作するコマンドセットの例としてＳＣＳＩコマンドを用いて説明する。尚、本発明は、ファイバチャネルとＳＣＳＩコマンドの組み合わせに限定されるものではなく、これらと同様に、ログイン、問い合わせ、ログアウトといった機能・機構を提供可能なプロトコルであればどのような組合せ、インタフェースであっても適用可能である。

【００１７】本発明の第一の実施例を以下に示す。初めに、ファイバチャネルのプロトコル上で本発明に関係する特徴を説明する。ファイバチャネルのインタフェースを持つ機器をノードと呼び、実際のインタフェースにあたる物理的な端子をポートと呼ぶ。ノードは１つ以上のポートを持つことが可能である。ファイバチャネルの系全体に同時に参加できるポートの数は、最大で２４ビットのアドレス数、すなわち、２の２４乗個（１６７７７２１６個）である。これらの接続を媒介するハードウェアをファブリックと呼ぶ。実際には、送信元および送信先のポートは、ファブリックを意識せずに互いのポートに関する情報のみを考慮して動作すればよい。

【００１８】各ノードおよびポートには、標準化団体（ＩＥＥＥ）から一定のルールによって割り当てられる、世界中でユニークな識別子が記憶されている。これは従来からＴＣＰ／ＩＰなどで馴染みのMACアドレスに相当するものであり、ハードウェア的に固定なアドレスである。このアドレスにはN_Ｐｏｒｔ_Ｎａｍｅ、Ｎｏｄｅ_Ｎａｍｅの２種類があり、それぞれ８バイトのサイズを持つ。N_Ｐｏｒｔ_Ｎａｍｅはポート毎に固有の値（ハードウェア・アドレス）であり、Ｎｏｄｅ_Ｎａｍｅはノード毎に固有の値（ハードウェア・アドレス）である。これらは、いずれも世界中でユニークな値であることから、ノードまたは、ポートを一意に識別できるアドレスとして、WWN（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｎａｍｅ）と呼ばれる。本特許の実施例では、WWNと記述した場合、N_Ｐｏｒｔ_Ｎａｍｅを指すものとする。

【００１９】ファイバチャネルでは、通信はＯｒｄｅｒｅｄ　Ｓｅｔと呼ばれる信号レベルの情報と、フレームと呼ばれる固定のフォーマットを持った論理的な情報とで行われる。図２はフレームの構造を示している。フレーム２０１は、フレームの始まりを示すＳＯＦ（Ｓｔａｒｔ　ｏｆ　Ｆｒａｍｅ）２０２と呼ばれる４バイトの識別子、リンク動作の制御やフレームの特徴づけを行う２４バイトのフレームヘッダ２０３、実際に転送される目的となるデータ部分であるデータフィールド２０４、４バイトの巡回冗長コード（ＣＲＣ）２０５、フレームの終わりを示すＥＯＦ（Ｅｎｄ　ｏｆ　Ｆｒａｍｅ）２０６と呼ばれる４バイトの識別子からなる。データフィールド２０４は０～２１１２バイトの間で可変である。

【００２０】次に、フレームヘッダの内容について説明する。２０７はフレームヘッダの構造について示している。ここではフレームヘッダ２０３の詳細構造２０７における、１ワード目の０～２３ビット領域にあたるS_ＩD２０８についてのみ説明する。S_ＩD（Ｓｏｕｒｃｅ　ＩD）２０８は当該フレームを送信するポートを識別するための３バイトのアドレス識別子であり、送受信されるすべてのフレームで有効な値を持つ。このS_ＩDは動的に変動する値であり、ファイバチャネルの規格セットの１つであるＦＣ_ＰＨでは、S_ＩDをファブリックによって、初期化手続き時に割り当てられる、としている。割り当てられる値は、それぞれのポートがもつN_Ｐｏｒｔ_Ｎａｍｅまたは、Ｎｏｄｅ_Ｎａｍｅに依存する。

【００２１】次に、ファイバチャネルプロトコルに基づく、送信元の機器と送信先の機器が通信に関して互いに情報を交換するログイン手続きについて述べる。図３は、送信元（ログイン要求元）３０１と送信先（ログイン受信先）３０２との間に取り交わされる情報のやりとりを示したものである。

【００２２】ファイバチャネルのログイン手続きには数種類存在するが、ここではクラス３のログインに関して述べる。ログイン要求元は、ＰＬＯＧＩフレーム３０３をログイン受信先へ送信する。このフレームには、ログ

イン要求元のN_Ｐｏｒｔ_Ｎａｍｅ、Ｎｏｄｅ_Ｎａｍｅ、Ｓ_ＩＤおよびその他の情報が含まれている。

【００２３】受信先の装置では、このフレームに含まれている情報を取り出し、ログインを承認する場合は、ＡＣＣ３０４と呼ばれるフレームをログイン要求元に対して送信する。一方、ログインを拒絶する場合は、ＬＳ_ＲＪＴ３０５と呼ばれるフレームをログイン要求元に対して送信する。

【００２４】ログイン要求元は、自らが送信したＰＬＯＧＩフレームに対してＡＣＣフレームの応答を検出すると、ログインが成功したことを知り、データ転送などのＩ／Ｏプロセスを開始できる状態となる。一方、ログイン要求元が、ＬＳ_ＲＪＴを受信した場合はログインが成立しなかったこととなり、当該ログイン受信先へのＩ／Ｏプロセスは実行不可となる。

【００２５】ここではクラス３のログインについて述べたが、他のログインプロセスにおいても、ログイン要求元からログイン受信先へ渡すことのできる情報の中に、Ｎ_Ｐｏｒｔ_Ｎａｍｅ、Ｎｏｄｅ_ＮａｍｅおよびＳ_ＩＤが含まれることにおいては同様である。

【００２６】次に、ＳＣＳＩコマンドセットでは必ずサポートされている標準的なコマンドである、Ｉｎｑｕｉｒｙコマンドについて説明する。Ｉｎｑｕｉｒｙコマンドとは、Ｉ／Ｏプロセスを開始するのに先立ち、Ｉ／Ｏプロセスの対象となる論理ユニットに対して、その実装状態、準備状態を問い合わせるコマンドである。図４は、ＳＣＳＩ規格で定義されたＩｎｑｕｉｒｙコマンドを、ファイバチャネル規格のフレームで送信する場合のデータフィールドの詳細構造を示している。フレーム、およびフレームヘッダの基本構造は図２と同様である。よって、Ｓ_ＩＤ４０５が含まれている。

【００２７】データフィールド４０３には４０６のＦＣＰ_ＣＭＮＤフォーマットに示すように、ＦＣＰ_ＬＵＮ４０７、ＦＣＰ_ＣＮＴＬ４０８、ＦＣＰ_ＣＤＢ４０９、ＦＣＰ_ＤＬ４１０と呼ばれる領域がある。ここではＦＣＰ_ＬＵＮ４０７、およびＦＣＰ_ＣＤＢ４０９について述べる。

【００２８】ＦＣＰ_ＬＵＮ４０７の中には、フレーム送信元が状態を問い合わせようとする、フレーム送信先のポートに関連付けられた論理ボリュームの識別子が格納されている。尚、論理ボリュームとは、目に見える単体としての記憶装置（物理ボリューム）に対して、便宜上仮想的に分割されナンバリングされた記憶領域をいう。また、この識別子をＬＵＮ（Ｌｏｇｉｃａｌ　Ｕｎｉｔ　Ｎｕｍｂｅｒ）という。

【００２９】ＦＣＰ_ＣＤＢ４０９の中には、ＳＣＳＩコマンドセットを使用する場合にはＳＣＳＩのコマンド記述ブロック（ＣＤＢ）と呼ばれる命令情報が格納される。このＦＣＰ_ＣＤＢ４０９の中に、ＳＣＳＩのＩｎｑｕｉｒｙコマンド情報が格納されて、前述のＦＣＰ_ＬＵＮ　４０７と共に、フレーム受信先へ情報が転送される。

【００３０】ＳＣＳＩコマンドセットでサポートされているその他のコマンド、例えば、Ｗｒｉｔｅコマンドや Ｒｅａｄコマンド等でも、フレームはＩｎｑｕｉｒｙコマンドと同様、４０１や４０６の構造である。したがって、本発明の実施に必須であるＳ_ＩＤやＦＣＰ_ＬＵＮを含むことは、それらのコマンドにおいても共通である。

【００３１】図５に、このＩｎｑｕｉｒｙコマンドを用いた論理ユニット問合せの手順を示す。論理ユニットにアクセスしようとするホストコンピュータ５０１は、アクセスしようとする論理ユニットをもつ記憶サブシステム５０２に対し、Ｉｎｑｕｉｒｙコマンドを格納したフレーム５０３を送信する。このフレームには、ホストコンピュータのＳ_ＩＤと、問合せを行う先の論理ユニットの識別子であるＬＵＮが含まれている。ここで、ＬＵＮについては、ＦＣＰ_ＬＵＮ領域の他に、ＦＣＰ_ＣＤＢ内のＩｎｑｕｉｒｙコマンド情報のフォーマット中にも設定することができる。どちらの値を使用しても得られる効果は同じであるが、本実施例ではＬＵＮの値はＦＣＰ_ＬＵＮ４０７に格納された値を使用するものとする。

【００３２】Ｉｎｑｕｉｒｙコマンドを含むフレームを受信した記憶サブシステム５０２は、問合せに対して必要なＩｎｑｕｉｒｙデータを準備し、作成したＩｎｑｕｉｒｙデータを含むフレーム５０４をホストコンピュータに送信する。このときＩｎｑｕｉｒｙデータを格納するフレームを、ＦＣＰ_ＤＡＴＡと呼ぶ。記憶サブシステムが、問合せのあった論理ユニットについて、クオリファイア０００（２進数）、デバイスタイプ００～０９（１６進数）のいずれかを設定する場合（５０４）、このＩｎｑｕｉｒｙデータを受信したホストコンピュータは、当該論理ユニットに対して、以降Ｉ／Ｏの発行が可能となる。

【００３３】一方、５０５に示すように、記憶サブシステムが、クオリファイア００１（２進数）または０１１（２進数）、デバイスタイプ１Ｆ（１６進数）を設定した場合、このＩｎｑｕｉｒｙデータ５０５を受信したホストコンピュータは、当該論理ユニットに対して、以降、Ｉ／Ｏの発行が不可能であることを認識する。以上のことから、Ｉｎｑｕｉｒｙデータに格納するクオリファイア、およびデバイス・タイプ・コードを、記憶サブシステム側でコントロールすれば、ホストコンピュータから記憶サブシステムの論理ユニットへのアクセス許可および不許可を制御できることが分かる。

【００３４】先に述べたように、Ｉｎｑｕｉｒｙコマンドの以外のＷｒｉｔｅコマンドやＲｅａｄコマンド等でも、基本的なフレームの作りは４０１のように共通である。したがって、送信先の記憶サブシステムが、送信元

のホストコンピュータが指定したＳ_ＩＤやＬＵＮが不正と検出すれば、アクセス拒否をすることが可能である。

【００３５】続いて、本発明の処理の流れについて詳細を述べる。図１は、本発明の実施例の装置構成を示したものである。記憶サブシステム１０１は、ファイバチャネル・インタフェース用のポート１０２～１０４を有し、ファイバチャネル・インタフェースを介して、ホストコンピュータ１０５～１０７と物理的に接続されている。ホストコンピュータ１０５～１０７もまた、ファイバチャネルインタフェース用のポート１０８～１１２を有しており、ホストコンピュータ１０５～１０７と記憶サブシステム１０１は、ファイバチャネル・プロトコルによる通信が可能となっている。ホストコンピュータには、１０５や１０６のように複数のファイバチャネル・ポートをもつものもあれば、１０７のように単一のファイバチャネル・ポートしかもたないものもある。記憶サブシステム１０１とホストコンピュータ１０５～１０７間のファイバチャネルインタフェースの接続形態（トポロジ）には、Ｐｏｉｎｔ_ｔｏ_Ｐｏｉｎｔや、アービトレーション・ループ接続、ファブリック接続等、いくつかの種類が存在するが、本発明はその接続形態には依存しないため、単にファイバチャネル１１３と記述する。

【００３６】まず、記憶サブシステム１０１は、種々の演算や処理を行うマイクロプロセッサ１１４を有し、複数の記憶装置群１１５、およびこれらにデータの読み書きを制御して行う記憶制御装置１１６、さらに記憶装置群１１５と記憶制御装置１１６を接続するためのパス１１７を有している。

【００３７】また、記憶サブシステム１０１は、種々の演算や処理のワーク領域として使用するメモリ１１８と、種々の管理情報、管理テーブル等を保存しておく不揮発メモリ１１９を有する。更に、ホストコンピュータへの応答を速くするための工夫として、キャッシュ１２０を有している。

【００３８】また、記憶サブシステム１０１は、通信制御部１２１を有し、通信回線１２２を介して、保守用端末装置１２３と接続されている。

【００３９】保守用端末装置１２３は、内部にマイクロプロセッサ１２４と、ユーザとのインタフェースとなる入力部１２５と処理の結果を出力する表示部１２６を有している。ユーザは、この入力部１２５を介して、本実施例で定義するいくつかのテーブルの設定を行うことができる。

【００４０】マイクロプロセッサ１１４、メモリ１１８、不揮発メモリ１１９、通信制御部１２１は図１のように、別個の構成としても良いし、記憶制御装置１１６の内部に配置しても良い。キャッシュ１２０の物理的形状（大きさ）により記憶制御装置１１６の内部に設けることができないときは、外部に所定のパス（経路）によって接続する。この場合には、ポート１０２～１０４の直下に記憶制御装置１１６が配置され、所定のパスにより各ポートと記憶制御装置１１６とが接続される構成となる。また、記憶制御装置１１６がマイクロプロセッサ１１４で為される機能を代替することも可能である。通信制御部１２１に接続される保守用端末装置１２３は、記憶サブシステム１０１の内部に設置しておくこと（常時接続）も、また、必要なときのみ通信回線１２２を介して接続すること（保守時接続）も可能である。

【００４１】図６において、本実施例の処理流れ概要を示す。手順６０１において、ユーザは前述の保守用端末装置１２３の入力部１２５を介して、記憶サブシステム内に存在する論理ユニット（ＬＵ）を規定するＬＵＮ（Ｌｏｇｉｃａｌ　Ｕｎｉｔ　Ｎｕｍｂｅｒ）と、そのＬＵＮにアクセスする可能性のあるホストコンピュータのWWN（Ｎ_Ｐｏｒｔ_Ｎａｍｅ）と、これらアクセスする可能性のあるホストコンピュータをユーザが任意にグループ化した際に割り当てるＧＩＤ（Ｇｒｏｕｐ　ＩＤ）を結びつけた「ＬＵＮアクセス管理テーブル」を作成する。本テーブルは、記憶サブシステム内の不揮発メモリ１１９に保持される。各ホストコンピュータには、本テーブルのＬＵＮが見える。各ホストコンピュータのWWNは既知である。

【００４２】手順６０２において、各ホストコンピュータが記憶サブシステムに対して、ファイバチャネル・プロトコルに基づいてログインしてくると、記憶サブシステムはＰＬＯＧＩフレームから、当該ホストコンピュータのWWNと、Ｓ_ＩＤを切り出し、同時に手順６０１でユーザが作成した「ＬＵＮアクセス管理テーブル」から当該のWWNが属するＧＩＤを検索し、それらの組み合わせを記述した「WWN_Ｓ_ＩＤ_ＧＩＤ変換テーブル」を作成し、不揮発メモリ１１９上にこれを保持する。

【００４３】「ＬＵＮアクセス管理テーブル」から、当該WWNが属するＧＩＤが検索されない場合は、ユーザが当該WWNの属するホストコンピュータ・グループを定義しなかったことを意味する。したがって、この場合は「WWN_Ｓ_ＩＤ_ＧＩＤ変換テーブル」の当該WWNに対応するＧＩＤには未定義のＩＤが登録される。記憶サブシステムはこの作業を全てのＰＬＯＧＩフレームに対して行う。

【００４４】手順６０３において、記憶サブシステムは、各ホストコンピュータが記憶サブシステム内の論理ユニットの状態を知るために送信したＩｎｑｕｉｒｙコマンドを含むフレームを受信する。このフレームを受信した記憶サブシステムは、そのフレームのヘッダからＳ_ＩＤを、データフィールドからＩｎｑｕｉｒｙコマンドの対象となるＬＵＮを切り出す。続いて、記憶サブシステムは、このＳ_ＩＤをキーにして上述の「WWN_Ｓ_ＩＤ_ＧＩＤ変換テーブル変換テーブル」を検索し、こ

のＳ_ＩＤに対応するＧＩＤを取得する。

【００４５】手順６０４において、記憶サブシステムは、得られたＧＩＤをキーにして上述の「ＬＵＮアクセス管理テーブル」から、Ｉｎｑｕｉｒｙコマンドの対象となっているＬＵＮを検索する。手順６０５では、手順６０４の結果、当該ＧＩＤに対応するＬＵＮを取得できたか否かの判定を行う。取得できた場合、すなわち当該ＧＩＤに対応するＬＵＮが「ＬＵＮアクセス管理テーブル」上に存在した場合は、当該ホストコンピュータの属するホストコンピュータ・グループによる当該ＬＵＮへのアクセスが許可される。一方、ＬＵＮが該テーブルに存在しない場合は、当該ホストコンピュータの属するホストコンピュータ・グループによる当該ＬＵＮへのアクセスは拒絶される。

【００４６】手順６０５の結果、当該ホストコンピュータによる当該ＬＵＮへのアクセスが許可される場合、記憶サブシステムは、手順６０６において、ホストコンピュータの発行したＩｎｑｕｉｒｙコマンドに対して、対象ＬＵが実装済みの設定（すなわちアクセス可能である旨の設定）を行った上で、Ｉｎｑｕｉｒｙデータを送信する。一方、当該ＬＵへのアクセスが拒絶される場合、記憶サブシステムは、手順６０７によって、ホストコンピュータの発行したＩｎｑｕｉｒｙコマンドに対して、対象ＬＵが未実装の設定、すなわちアクセス不可である旨の設定を行った上で、Ｉｎｑｕｉｒｙデータを送信する。

【００４７】Ｉｎｑｕｉｒｙデータを受信したホストコンピュータは、そのフレームを解析し、解析の結果、記憶サブシステムの当該仮想ＬＵＮへのアクセスが許可されたことを認識すると、ホストコンピュータは以降、当該ＬＵＮに対して、コマンド（Ｉ／Ｏ要求）を継続して発行することができる。この場合、手順６０８にあるように、記憶サブシステムは当該ホストコンピュータからのログインが有効である間は、当該ＬＵへのコマンド受信を継続することができる。

【００４８】一方、当該ＬＵＮへのアクセスが拒否されたことを認識したホストコンピュータは、記憶サブシステムへのログインが有効である間、当該ＬＵへ再度アクセスすることはない。以下、上記の記憶サブシステム内の特定ＬＵＮに対するホストコンピュータからのアクセス可否を制御する方法を、「本発明におけるＬＵＮセキュリティ」と呼ぶ。

【００４９】次に、図７から図１０を用いてもう少し詳細に技術的課題を説明し、図１１から本発明について説明する。はじめに、上記手順６０１の「ＬＵＮアクセス管理テーブル」の作成について記述する。本発明におけるＬＵＮセキュリティは、記憶サブシステムのもつポート毎に管理され、ホストコンピュータは、この記憶サブシステムのポートを通して、記憶サブシステム内のＬＵにアクセスするものとする。この場合、最も簡単な方法として、ホストコンピュータを一意に識別する情報であるWWNと、当該ホストコンピュータにアクセスを許可するＬＵＮの対応を定義した、図７に示すようなテーブル７０１を、記憶サブシステム内に設ければよい。このことは、ホストコンピュータと記憶サブシステムとが専用の回線で接続されている場合には何ら問題なく、その機能を達成することとなる。

【００５０】テーブル７０１は、記憶サブシステム内の記憶領域に対して、単一ポート配下で一意にナンバリングし、その論理ユニット番号（ＬＵＮ）を、そのままホストコンピュータのWWNに対して割り当てている。図７では、WWN７０２のホストコンピュータには、ＬＵ０～２にのみアクセスが許可され、WWN７０３のホストコンピュータは、ＬＵ３、４、および７にのみアクセスが許可され、WWN７０４のホストコンピュータは、ＬＵ５～６にのみアクセスが許可されている。

【００５１】したがって、例えばＬＵ０～２は、WWN７０２のホストコンピュータ以外のホストコンピュータからは、アクセス不可となり、本発明におけるＬＵＮセキュリティが実現されるからである。

【００５２】しかし、ホストコンピュータと記憶サブシステム間に、ファイバチャネル対応のハブや、スイッチなどの機器類が介在するような最近の複雑な使用環境下では、７０１のテーブルだけでは不十分である。今日、多くのホストコンピュータでは、接続されている記憶サブシステムのＬＵ０にアクセスできない場合には、そのＬＵ０以降の同系列のＬＵ（ＳＣＳＩ-２の規格では、この１系列は８つのＬＵで構成されるため、ＬＵ０～ＬＵ７までが同系列となる。）には全く存在の問い合わせをしない、とするものが多いためである。このようなホストコンピュータからアクセスがあった場合、テーブル７０１のような規定方法では、ホストコンピュータ７０３や７０４は、アクセスを許可するＬＵＮがそれぞれ規定されていながら、ＬＵ０にアクセスできないために、テーブル７０１で規定したアクセス許可のＬＵＮを参照できない事態が発生してしまう。併せて、このような現象は、ディスクアレイ装置のような記憶資源を豊富に提供し得る装置においては、著しくその利用率を下げ、記憶資源の無駄を生ずる。

【００５３】そこで、これを防ぐためにホストコンピュータ７０３、７０４にＬＵ０へのアクセスを許可すると、ＬＵ０の排他がなくなりセキュリティが保証されない。仮にこれを認めた場合にも、ホストコンピュータ７０３と７０４が異なるＯＳをもつホストコンピュータである場合、ＬＵ０を共有することは、それぞれのＯＳによるフォーマットの違いから困難でとなってしまう。

【００５４】一方、図７において、記憶サブシステムの当該ポート配下にＬＵ０の定義がなくても、全てのＬＵＮに対して存在の問い合わせを行うことが可能な、WWN７０５～７０７を持つホストコンピュータ群が存在す

ると仮定する。ここでは、WWN７０５のホストコンピュータは、ＬＵ０、１、７にのみアクセスが許可され、WWN７０６のホストコンピュータは、ＬＵ３、５、６にのみアクセスが許可され、WWN７０７のホストコンピュータは、ＬＵ２、４にのみアクセスが許可されている。

【００５５】この状態を視覚的に表したのが図８である。ホストコンピュータ８０２～８０４は、図７WWN７０５～７０７を持つホストコンピュータに相当する。ホストコンピュータ８０２～８０４は、ファイバチャネル対応のハブ、スイッチ又はルーター８０５を経由して記憶サブシステムの同一のポート８０６に接続している。このような使用環境において、各々のホストコンピュータ８０２～８０４に対し、無計画にアクセス対象ＬＵＮを定義したり、以前割り当てたＬＵＮと異なるＬＵＮをアクセス対象として割り当てた場合、記憶サブシステム内の同一ポート配下で一意にナンバリングしたＬＵＮをそのままホストコンピュータに開示している８０１のような記憶サブシステムではＬＵＮの開示方法に柔軟性がなく、当該ポート配下が、ＬＵ群８０７のようにＬＵが離散した状態で見え、使用上、著しく管理しにくい状態となってしまう。

【００５６】一方、最近、記憶サブシステムの１つのポート配下に９個以上のＬＵを定義しても、これを認識するホストコンピュータが存在するが、このようなホストコンピュータと従来のように１つの記憶サブシステムのポート配下にＬＵ０～７までの８個のＬＵしかサポートしないホストコンピュータ間でＬＵＮセキュリティを実施した場合の問題点を示す。

【００５７】図９において、WWN９０２、９０４を持つホストコンピュータが、接続する記憶サブシステムのポート配下にＬＵ０が存在しなくても、各ＬＵに存在の問い合わせを行う機構をもち、かつ、接続する記憶サブシステムのポート配下にＬＵを１６個まで認識する場合について以下説明する。

【００５８】WWN９０３を持つホストコンピュータは、接続する記憶サブシステムのポート配下にＬＵ０が存在しなくても、各ＬＵに存在の問い合わせを行えるが、サポート可能なＬＵはＬＵ０～７の範囲の８個までとする。テーブル９０１から分かるように、WWN９０２を持つホストコンピュータはＬＵ０～５の範囲でアクセスが許可されており、WWN９０３を持つホストコンピュータはＬＵ６～１０の範囲で、またWWN９０４を持つホストコンピュータはＬＵ１１～１５の範囲でアクセスが許されている。この状態を視覚的に表したのが図１０である。

【００５９】ホストコンピュータ１００２～１００４は、図９のWWN９０２～９０４を持つホストコンピュータに相当する。ホストコンピュータ１００２～１００４は、ファイバチャネル対応のハブ、スイッチ又はルーター１００５を経由して記憶サブシステムの同一のポート１００６に接続している。このような使用環境において、各々のホストコンピュータ１００２～１００４に対して、ＬＵ群１００８のように記憶サブシステム内のＬＵを割り当てたとすると、ホストコンピュータＡ１００２には、ＬＵ群１００８中のＬＵ０～５の範囲のみアクセス許可対象として見え、ホストコンピュータＣ１００４には、ＬＵ群１００８中のＬＵ１１～１５の範囲のみアクセス許可対象として見え、それぞれＬＵＮセキュリティの目的を果たすことができる。しかし、ホストコンピュータＢ１００３は、元々１ポート配下にＬＵ０～７までの範囲で、８個までしかＬＵを認識できないため、ＬＵ群１００７の範囲内でしか問い合わせを実施することができない。よって、テーブル９０１において、ＬＵ６～１０までアクセス許可をしても、実際には、ＬＵ６、７にしかアクセスできないという問題が生じる。これも、記憶サブシステム内の同一ポート配下で一意にナンバリングしたＬＵをそのまま開示しているために起こる弊害である。

【００６０】以上のような懸念を考慮して、本発明では、図１１に示すような「ＬＵＮアクセス管理テーブル」１１０１を定義する。テーブル１１０１は、図７のテーブル７０１、図９のテーブル９０１のように記憶サブシステム内の同一ポート配下で一意にナンバリングしたＬＵＮを単にWWNに直接割り当てたテーブルとは異なる。

【００６１】テーブル１１０１は、アクセスする可能性のあるホストコンピュータのWWNと、これらホストコンピュータ群をユーザが任意にグループ化した際に割り当てるＧＩＤ（Ｇｒｏｕｐ　ＩＤ）を結びつけ、これらホストコンピュータ・グループに対して、記憶サブシステム内のアクセスを許可できる記憶領域に、ユーザが任意に設定できる論理ユニット番号（ＬＵＮ）を付与するものである。

【００６２】本テーブルは、記憶サブシステムのポート単位に作成される。この「ＬＵＮアクセス管理テーブル」１１０１を定義した記憶サブシステムでは、ユーザが任意にグループ化したホストコンピュータ群に対して、ユーザの使用希望に沿った形でＬＵＮを柔軟にナンバリングし、それらを開示することができる。

【００６３】通常、ＯＳが異なると、ＬＵに対する論理フォーマットが異なるため、異ＯＳ間でのＬＵの共有はできない。したがって、「ＬＵＮアクセス管理テーブル」１１０１において、ユーザが登録するグループは、通常、同一のＯＳを搭載したホストコンピュータ群となる。

【００６４】このホストコンピュータ・グループ登録において、ユーザの使用希望条件（例えば、交替パス構成、ホストコンピュータ間のクラスタ構成等）をより詳細に組み込めば、更にユーザの使い勝手を向上させるこ

とができ、同時に記憶サブシステム内の記憶領域を有効利用することができる。 「ＬＵＮアクセス管理テーブル」１１０１の詳細な設定例を図１１を用いて説明する。１１０１において、WWN１１１２～WWN１１１４をもつホストコンピュータ群は、同一のＯＳ種１を搭載し、ＧｒｏｕｐＡ １１０５としてカテゴライズされている。これらのホストコンピュータ・グループには記憶サブシステム内のＬＵ０～３へのアクセスが許可されている。記憶サブシステム内では、これらＬＵ０～３には記憶領域番号０～３（以下、適宜、記憶領域＃０～３と略記する）が割り当てられている。

【００６５】また、 WWN１１１５～WWN１１１７をもつホストコンピュータ群は、同一のＯＳ種２を搭載し、ＧｒｏｕｐＢ １１０６にカテゴライズされている。これらホストコンピュータ・グループには、やはりＬＵ０～３がアクセス許可されているように見えるが、記憶サブシステムの内部ではこれらＬＵ０～３には、記憶領域＃６０～６３が割り当てられており、上述のＧｒｏｕｐＡ １１０５の使用記憶領域とは排他がなされており、本発明におけるＬＵＮセキュリティが実現されている。

【００６６】一方、 WWN１１１８～WWN１１２１をもつホストコンピュータ群は、ＧｒｏｕｐＣ１１０７にカテゴライズされているが、その内訳は、ＯＳ種３を搭載したホストコンピュータ群とＯＳ種４を搭載したホストコンピュータ群の混在である。通常、ＯＳ種が異なると論理フォーマットが異なるため、ＬＵの共有ができないが、共有可能な異なるＯＳ種が存在する場合、このようなグループ化も可能である。、 ＧｒｏｕｐＣ １１０７には、ＬＵ０～５が連続してアクセス許可されているように見えるが、実際には離散した記憶領域＃７、１１、７０、７９、８７、１１９が割り当てられている。

【００６７】また、WWN１１２２、１１２３をもつホストコンピュータ群は、ＧｒｏｕｐＤ １１０８にカテゴライズされているが、それぞれＯＳ種５、ＯＳ種６という異なるＯＳ種を搭載している。 ＧｒｏｕｐＤ １１０８のホストコンピュータ群は、アクセスするポート配下にＬＵ０が存在しなくても、その他のＬＵを離散的に認識する先進的なアーキテクチャをもっているため、ＬＵ５０、ＬＵ５１、ＬＵ６２という複雑な開示方法でアクセス可能なＬＵが定義されている。これらアクセス可能なＬＵには、それぞれ記憶領域＃４０、９９、１００が割り当てられている。

【００６８】「ＬＵＮアクセス管理テーブル」１１０１へのグループ登録は、必ずしも複数ホストコンピュータから成る必要はない。例えば、WWN１１２４のホストコンピュータに対して、単独でアクセス許可するＬＵを規定したい場合、ホストコンピュータ１台からなるＧｒｏｕｐＥ １１０９を登録すればよい。このような登録方法により、アクセス許可するホストコンピュータの分解能を上げることができる。 ＧｒｏｕｐＥ １１０９には、ＬＵ０～１へのアクセスが許可され、そこには記憶領域＃４、５が割り当てられている。

【００６９】また、最近のＳＡＮ環境において問題となっている制限に対する解決策を示す。WWN１１２５および、１１２６のホストコンピュータは、共に単一ポート配下に２５６個のＬＵまでしか認識できないＯＳ種７として、ＧｒｏｕｐＦ １１１０にカテゴライズされている。しかし、実際には単一ポート配下で５１２個のＬＵを認識させたいというユーザ要求があると仮定する。この場合、WWN１１２５および、１１２６のホストコンピュータを別グループＧｒｏｕｐＧ １１１１として再度登録する。 両ホストコンピュータは、いずれも２５６個のＬＵまでしか認識しないため、 ＧｒｏｕｐＦ １１１０にはＬＵ０～２５５まで、ＧｒｏｕｐＧ １１１１にもＬＵ０～２５５までをアクセス許可ＬＵとして定義する。ただし、ＧｒｏｕｐＦ １１１０のＬＵ０～２５５には記憶領域＃０～２５５を、ＧｒｏｕｐＧ １１１１のＬＵ０～２５５には記憶領域＃２５６～５１２を割り当てることにより、ホストコンピュータの既存の処理、制限その他の機能を変更せずに、５１２個のＬＵを開示しながら、本発明におけるＬＵＮセキュリティ機能を実現している。

【００７０】最後に、上記とは異なる設定パターンを示す。WWN１１２９とWWN１１３０のホストコンピュータとWWN１１３１とWWN１１３２のホストコンピュータは、同一のＯＳ種８を搭載した異なるフロアに存在するホストコンピュータである。これらのホストコンピュータを相手にする管理者は、これら４つのホストコンピュータに、異なるアクセスＬＵＮでファイルやアプリケーションを開示したいが、開示する実体は同じ記憶領域の同じ内容としたい、と仮定する。そのような場合、テーブル１１０１のＧｒｏｕｐＨ１１２７とＧｒｏｕｐＩ１１２８のような設定を実施すればよい。この場合、ＧｒｏｕｐＨ１１２７にはＬＵ０、１が開示され、ＧｒｏｕｐＩ１１２８には、ＬＵ４、５が開示されるが、実際の参照先記憶領域＃は同一の１０、１１である。これら以外のホストコンピュータからのアクセスは拒絶される。これにより、上記管理者の目的にそった本発明におけるＬＵＮセキュリティ機能を提供することができる。

【００７１】以上、本発明の「ＬＵＮアクセス管理テーブル」によるホストコンピュータのグループ化とＬＵＮの対応づけについて具体的に説明したが、これを視覚的に表すと図１３のようになる。対応する「ＬＵＮアクセス管理テーブル」１２０１を図１２に示した。

【００７２】テーブル１２０１において、各ホストコンピュータ・グループ１２０５～１２０７にアクセスを許可したＬＵ群１２０４は、実際には図１３の記憶領域群１３０３のように全く乱雑な配置をとっている。しか

し、これをテーブル１２０１のＬＵ群１２０４にマッピングすることで、図１３のＬＵ群１３０２の状態となり、ホストコンピュータグループ１３０７～１３０９に記憶サブシステム内の実際の記憶領域群の配置状態１３０３を意識させない状態でＬＵを開示することができる。尚、図１３におけるホストコンピュータグループ１３０７～１３０９は、図１２におけるホストコンピュータ・グループ１２０５～１２０７に相当している。

【００７３】これにより、ホストコンピュータの既存の処理、制限その他の機能を変更せずに、本発明におけるＬＵＮセキュリティが実現でき、記憶サブシステム資源の柔軟かつ効率的な運用も可能となる。

【００７４】更に、このようなホストコンピュータのグループ化を実現することにより、記憶サブシステム１３０１内の単一ポート配下でありながら、ホストコンピュータ・グループ毎に記憶サブシステムとの接続インタフェース情報１３１０～１３１２（図１３）を設定することができる。

【００７５】接続上のインタフェース情報とは、例えば、記憶サブシステムの受領Ｉ／Ｏ、受領キューの深さであったり、Ｉｎｑｕｉｒｙの応答内容等を指す。従来の記憶サブシステムでは、単一ポート配下のインタフェース情報は単一であるのが一般的であった。

【００７６】本発明の「ＬＵＮアクセス管理テーブル」１１０１や１２０１は、図１４の手順１４０１～１４０３に示すように、記憶サブシステムの全ポートに対して定義された後、記憶サブシステム内の不揮発メモリに保持される。不揮発メモリに保持されることで、本テーブルは、記憶サブシステムの電源切断によっても消失しない。また、所定の記憶装置１１５（記憶装置１０１、図１）に格納しても良い。

【００７７】続いて、記憶サブシステムがホストコンピュータからログインされる際の処理について説明する。本実施例では、一連のログイン処理を通じて、ホストコンピュータを一意に識別するWWNからＧＩＤ（グループＩＤ）取得し、ログイン以降に使用されるホストコンピュータを一意に識別するＳ＿ＩＤとＧＩＤを対応させる。

【００７８】ホストコンピュータが起動すると、図１５の手順１５０１において、記憶サブシステムは、ＰＬＯＧＩフレームを受信する。ＰＬＯＧＩフレームを受信した記憶サブシステムは、手順１５０２において、フレームヘッダからホストコンピュータのＳ＿ＩＤを、手順１５０３において、データフィールドからホストコンピュータのWWN（Ｎ＿Ｐｏｒｔ＿Ｎａｍｅ）を取得する。続いて、記憶サブシステムは手順１５０４において、このWWNとＳ＿ＩＤとＧＩＤ（グループＩＤ）を図１６に示す「WWN_S_ID_GID変換テーブル」１６０１に記録作成し、これを手順１５０５において、記憶サブシステム内の不揮発メモリに保持する。ここでＧＩＤは、先に述べた、ユーザが設定する「ＬＵＮアクセス管理テーブル」からWWNをキーに検索することで得られる。「WWN_S_ID_GID変換テーブル」１６５０１は、記憶サブシステムのポート毎に作成される。

【００７９】このテーブルに登録されたWWNをもつホストコンピュータから、以後、コマンドが送信されると、記憶サブシステムはそのフレームヘッダからＳ＿ＩＤを取得し、「WWN_S_ID_GID変換テーブル」１６０１を使用して、そのＳ＿ＩＤに対応するＧＩＤを知ることができる。記憶サブシステムは、この「WWN_S_ID_GID変換テーブル」を不揮発メモリ上に保存すると、手順１５０６において、当該ホストコンピュータのログインを承認した旨のＡＣＣフレームを送信する。記憶サブシステムからＡＣＣフレームを受信したホストコンピュータは、これ以降、記憶サブシステムに対してＩｎｑｕｉｒｙコマンドを発行することができる。

【００８０】続いて、ホストコンピュータからのＩｎｑｕｉｒｙコマンド受信と、これに対する記憶サブシステムのセキュリティ応答について説明する。図１７、図１８は、この一連の処理の流れを示したものであり、図１９は、この一連の処理の流れにおいて使用される各テーブルやパラメータの参照関係を示したものである。

【００８１】図１７の手順１７０１において、記憶サブシステムは、ホストコンピュータからファイバチャネルに規定されたＦＣＰ_CMNDフレームを受信する。すると記憶サブシステムは、手順１７０２において、そのＦＣＰ_CMNDのデータフレームの内容を解析する。

【００８２】続いて記憶サブシステムは、手順１７０３において、当該のＦＣＰ_CMNDの内容がＩｎｑｕｉｒｙコマンドであるか否かをチェックする。Ｉｎｑｕｉｒｙコマンドでない場合、記憶サブシステムは手順１７０４において、そのコマンドに対応した処理を実行する。一方、Ｉｎｑｕｉｒｙコマンドであった場合、記憶サブシステムは手順１７０５において、当該ＦＣＰ_CMNDフレームのヘッダからホストコンピュータのＳ＿ＩＤを取得し、手順１７０６において、当該ＦＣＰ_CMNDフレームのデータフィールドのＦＣＰ_ＬＵＮから対象とするＬＵＮを取得する。

【００８３】引き続き、記憶サブシステムは手順１７０７において、得られたＳ＿ＩＤをキーにして、図１６の「WWN_S_ID_GID 変換テーブル」１６０１を検索し、このＳ＿ＩＤに対応するＧＩＤを取得する。ここまでの流れは、図１９の手順１９０１、１９０２、１９０３の参照動作を指す。

【００８４】手順１９０３において、当該Ｓ＿ＩＤに対するＧＩＤがテーブル１６０１で検索されない場合、当該ホストコンピュータにアクセス許可されたＬＵＮはユーザによって登録されてなかったこととなり、当該ホストコンピュータからリクエストされたＬＵＮへのアクセスは拒絶される。

【００８５】続いて、手順１７０８（図１７）において、このＧＩＤに対してアクセス許可されているＬＵＮ情報を取得する。そして、手順１８０１（図１８）において、このＧＩＤをもつホストコンピュータのＩｎｑｕｉｒｙコマンドから得られたＬＵＮが、「ＬＵＮアクセス管理テーブル」上でアクセス許可されたＬＵＮとして登録されているか否かを判定する。ここまでの流れは、図１９の手順１９０４および１９０５の参照動作を指す。

【００８６】手順１９０４～１９０５における参照動作では、ＧＩＤをキーに、Ｓ_ＩＤからアクセス許可されたＬＵＮを検索しているが、このＧＩＤは個々のＷＷＮをグループ化してまとめた属性であるため、一般に、ＧＩＤ：アクセス許可されるＬＵＮ＝多：１の関係となる。これは、従来のＷＷＮをキーにしたＬＵＮセキュリティのＷＷＮ：アクセス許可されるＬＵＮ＝１：１の関係よりも、ホストコンピュータ側の分解能が下がる分、検索動作が簡易になり一般に高速である。

【００８７】「ＬＵＮアクセス管理テーブル」（図１１、図１２）の当該エントリに、手順１７０６で得られたＬＵＮが登録されている場合、当該ホストコンピュータからそのＬＵＮへのアクセスが許可されるため、記憶サブシステムは手順１８０２（図１８）において、ホストコンピュータ応答用Ｉｎｑｕｉｒｙデータのクオリファイアに２進数の'０００'を、デバイスタイプに記憶サブシステムのデバイスタイプコードをセットする。

【００８８】一方、「ＬＵＮアクセス管理テーブル」の当該エントリに、手順１７０６で得られたＬＵＮが仮想ＬＵＮとして登録されていない場合、当該ホストコンピュータからその仮想ＬＵＮへのアクセスは拒絶されるため、記憶サブシステムは手順１８０３において、ホストコンピュータ応答用Ｉｎｑｕｉｒｙデータのクオリファイアに２進数の'００１'または、'０１１'を、デバイスタイプに１６進数の'１Ｆ'をセットする。

【００８９】次に記憶サブシステムは、手順１８０４において、ＦＣＰ_ＤＡＴＡフレームに上記の応答用Ｉｎｑｕｉｒｙデータをセットして、ホストコンピュータへ送信する。続いて記憶サブシステムは、手順１８０５において、ホストコンピュータのＩｎｑｕｉｒｙコマンドの応答を完了したことを示すＦＣＰ_ＲＳＰフレームを送信する。

【００９０】図１８の手順１８０２、１８０４に引き続いて、Ｉｎｑｕｉｒｙデータを含むＦＣＰ_ＤＡＴＡを記憶サブシステムから受信したホストコンピュータは、当該ＬＵＮへのアクセスは可能と判断し、以降、当該ＬＵＮへのアクセス可否を再度問い合わせることなく、アクセスを継続することができる。ここで、当該ホストコンピュータがアクセスするＬＵＮは、実際にはＬＵＮと一意に対応づけられた記憶サブシステム内の記憶領域＃となる。

【００９１】一方、手順１８０３、１８０４に引き続いて、Ｉｎｑｕｉｒｙデータを含むＦＣＰ_ＤＡＴＡを記憶サブシステムから受信したホストコンピュータは、当該ＬＵＮへのアクセスは不可能と判断し、以降、当該ＬＵＮへのアクセス可否を再度問い合わせることはなく、アクセスもしない。

【００９２】本実施例では、上記したようにホストコンピュータがアクセス可否を当該ＬＵＮへ問い合わせるのは、Ｉｎｑｕｉｒｙコマンド発行時だけである。つまり、ログインが有効である間は、この問い合わせを繰り返し行う必要がない。これにより、ホストコンピュータと記憶サブシステム間のデータ転送効率を落とすことなく、強固なＬＵＮセキュリティを実現できる。

【００９３】尚、ＬＵＮから記憶サブシステム内の記憶領域＃へのマッピングに「記憶領域＃＝ｆ（ＧＩＤ、ＬＵＮ）」という相関関係をもたせた関数ｆとすれば、有効なＧＩＤかつＬＵＮ値に対しては有効な記憶領域＃が出力され、それ以外に対しては有効な記憶領域＃が出力されないこととなる。

【００９４】ここでｆ（ｎ、ｍ）は、ＧＩＤとＬＵＮをパラメタに、ホストコンピュータに開示されたＬＵＮを記憶サブシステム内の記憶領域＃にマッピング変換する関数である。これにより、Ｉｎｑｕｉｒｙコマンド以降のＷｒｉｔｅコマンドやＲｅａｄコマンドにおいて、手順１９０１～１９０５の検索動作を伴わずに、指定ＬＵＮから記憶領域＃への変換動作中にアクセス可否チェックを最小限のオーバーヘッドで行うことができる。

【００９５】以上のように、同一ポート配下で複数ホストコンピュータ群をグループ化して扱い、そのグループ単位にＬＵの割当てをユーザが任意に選択・設定可能な方法で実施することにより、ホストコンピュータ側の既存の処理、制限その他の機能を変えることなく、ＬＵＮセキュリティを高速な判定ロジックと記憶サブシステム内の記憶領域高効率使用と共に実現することができる。

【００９６】本実施例では、ファイバチャネルを例に説明したが、実施においては、必ずしもファイバチャネルに限定する必要はなく、同等機能を提供可能なプロトコル環境であれば、その種別は問わない。また、記憶サブシステムに関しても、本実施例では、主にディスクアレイ装置を想定して記述しているが、通常の磁気ディスク装置や、記憶装置を媒体可換の光ディスクライブラリや、テープライブラリなどに置換することも可能である。

【００９７】更には、最近のＳＡＮ環境の仮想化（Ｖｉｒｔｕａｌｉｚａｔｉｏｎ）を考慮して、本発明を複数の記憶サブシステム間で実施してもよい。この場合、前記の各テーブルの定義・設定事項は、１つの記憶サブシステム上で実施され、その他の記憶サブシステム内の論理ユニットに、その定義・設定が及ぶよう連絡通信経路を設け、１つの記憶サブシステムで集中して制御するよ

う構成する。

【００９８】また、このような集中制御およびそれに必要なテーブルの定義は、必ずしも特定の記憶サブシステム上で行う必要はなく、複数の記憶サブシステムとＦｉｂｒｅＣｈａｎｎｅｌその他共通インタフェースで接続され、複数の記憶サブシステム内の論理ユニットが認識可能であれば、ホストコンピュータ上のプログラム処理、またはスイッチング・ハブやルータ上の内部処理にもたせてもよい。このようにＦｉｂｒｅＣｈａｎｎｅｌ等のネットワークで結合された複数の記憶サブシステム間で本発明におけるＬＵＮセキュリティを実現する場合では、アクセス許可された論理ユニットを内包した記憶サブシステム群と、ホストコンピュータ・グループと接続するポートをもつ記憶サブシステムやスイッチ、ルータは、同一筐体に属している必要はない。

【００９９】

【発明の効果】コンピュータの既存の処理、制限その他の機能を変更せずに、記憶サブシステム内の管理テーブルを用いることによって、ユーザが任意にグループ化したホストコンピュータ群に、ユーザの運用希望に沿った形式で、記憶サブシステム内の論理ユニットを開示し、そのグループ単位で記憶サブシステム内のＬＵに対するアクセス可否を制限し、同時に、そのグループ単位に接続上のインターフェース設定が可能なセキュリティ機能を記憶サブシステムの単一ポート配下で提供することができる。

【０１００】更に、記憶サブシステム内のＬＵに対するアクセス可否判定は、Ｉｎｑｕｉｒｙコマンドのような問合せコマンド発行時点で判明するため、それ以降この判定を繰り返す必要がないため、記憶サブシステムを高い性能で維持運用しながら、ＬＵに対する強固なセキュリティ機能を確保することができる。

【図面の簡単な説明】

【図１】本発明の実施の形態におけるハードウェアの構成図である。

【図２】本発明の実施の形態におけるフレーム・フォーマットおよびそのフレーム・ヘッダの詳細を示す図である。

【図３】本発明の実施の形態におけるログインプロセスを示す図である。

【図４】本発明の実施の形態におけるＩｎｑｕｉｒｙコマンド送信時のフレーム・フォーマットの詳細を示す図である。

【図５】本発明の実施の形態におけるＩｎｑｕｉｒｙコマンドによる論理ユニットへのアクセス問合せシーケンスを示す図である。

【図６】本発明の実施の形態におけるＬＵＮセキュリティの処理シーケンス概要を示すフローチャートである。

【図７】本発明を利用しないことによる不完全な「ＬＵＮアクセス管理テーブル」のフォーマットおよび、その第一の例を示す図である。

【図８】図７の状態を視覚的に示した図である。

【図９】本発明を利用しないことによる不完全な「ＬＵＮアクセス管理テーブル」のフォーマットおよび、その第２の例を示す図である。

【図１０】図９の状態を視覚的に示した図である。

【図１１】本発明の実施の形態における「ＬＵＮアクセス管理テーブル」のフォーマットおよび、その第一の利用例を示す図である。

【図１２】本発明の実施の形態における「ＬＵＮアクセス管理テーブル」のフォーマットおよび、その第２の利用例を示す図である。

【図１３】本発明の実施の形態におけるＬＵＮセキュリティの効果を視覚的に示した図である。

【図１４】本発明の実施の形態における「ＬＵＮアクセス管理テーブル」の作成シーケンスを示すフローチャートである。

【図１５】本発明の実施の形態における「WWN_S_ID_GID変換テーブル」の作成シーケンスを示すフローチャートである。

【図１６】本発明の実施の形態における「WWN_S_ID_GID変換テーブル」のフォーマットの第一の利用例を示す図である。

【図１７】本発明の実施の形態におけるＬＵＮセキュリティのホストコンピュータ送信のＩｎｑｕｉｒｙコマンドに対するＬＵＮアクセス可否判定シーケンスを示すフローチャートである。

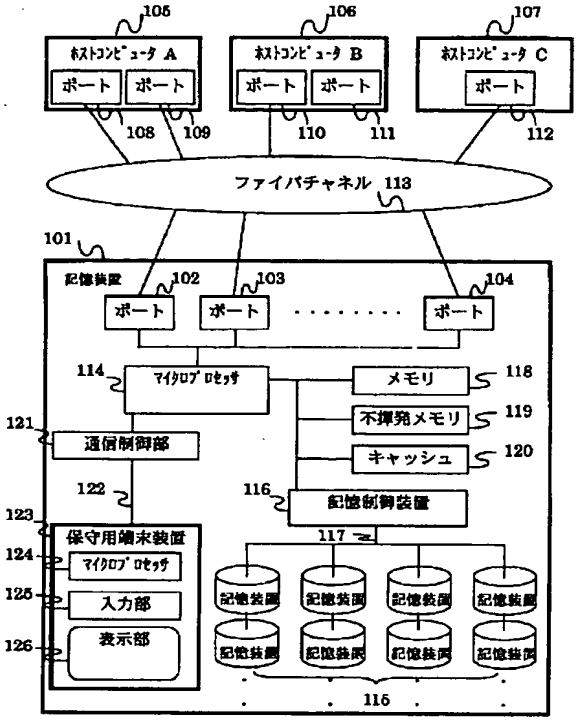
【図１８】図１７のフローチャートの続きを示すフローチャートである。

【図１９】本発明の実施の形態におけるＬＵＮセキュリティの各テーブル間の参照関係を示す図である。

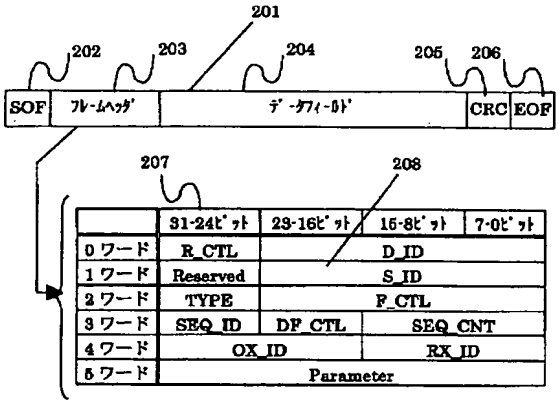
【符号の説明】

１０１……発明実施形態におけるハードウェア構成図、２０１……フレーム・フォーマット、　２０７……フレーム・ヘッダの詳細、２０８……S_ID、４０６……FCP_CMNDフレーム・フォーマット、７０４……不完全な「ＬＵＮアクセス管理テーブル」の第１の例、８０１……記憶サブシステム、９０１……不完全な「ＬＵＮアクセス管理テーブル」の第２の例、１００１……記憶サブシステム、１１０１……「ＬＵＮアクセス管理テーブル」の第１の例、１２０１……「ＬＵＮアクセス管理テーブル」の第２の例、１３０１……記憶サブシステム、１３０２……記憶サブシステムのポート配下に定義されたＬＵ群ＬＵＡ０～ＬＵＡ４、ＬＵＢ０～ＬＵＢ２、ＬＵＣ０～ＬＵＣ３、１６０１……「WWN_S_ID_GID変換テーブル」の第一の例。

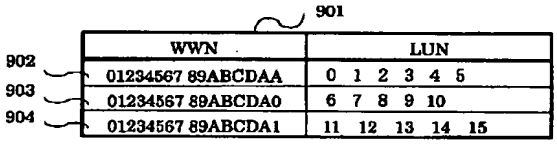
【図１】


105
106
107
ホストコンピュータ A
ホストコンピュータ B
ホストコンピュータ C
ポート
108
109
110
111
112
ファイバチャネル 113
101
記憶装置
102
103
104
114
マイクロプロセッサ
メモリ
118
不揮発メモリ
119
キャッシュ
120
121
通信制御部
122
116
記憶制御装置
117
123
保守用端末装置
124
マイクロプロセッサ
125
入力部
126
表示部
記憶装置
116

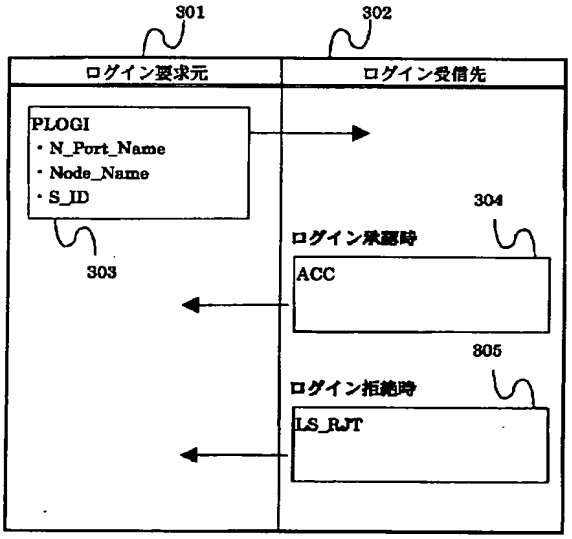
【図２】


201
202
203
204
205
206
SOF
フレームヘッダ
データフィールド
CRC
EOF
207
208
31-24ビット
23-16ビット
15-8ビット
7-0ビット
0 ワード
R_CTL
D_ID
1 ワード
Reserved
S_ID
2 ワード
TYPE
F_CTL
3 ワード
SEQ_ID
DF_CTL
SEQ_CNT
4 ワード
OX_ID
RX_ID
5 ワード
Parameter

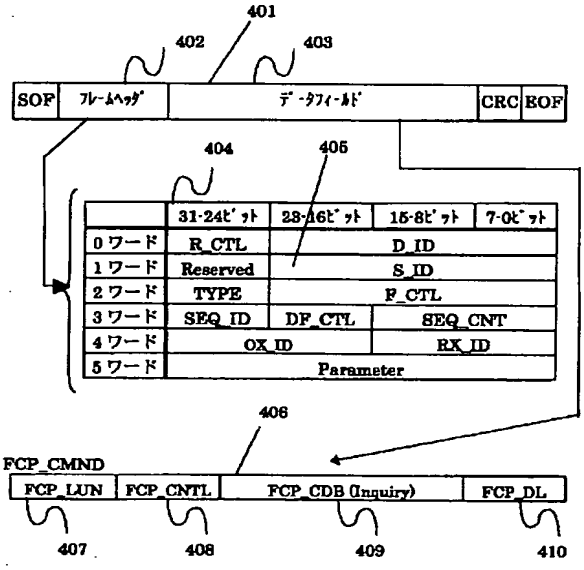
【図９】


901
WWN
LUN
902
01234567 89ABCDAA
0 1 2 3 4 5
903
01234567 89ABCDA0
6 7 8 9 10
904
01234567 89ABCDA1
11 12 13 14 15

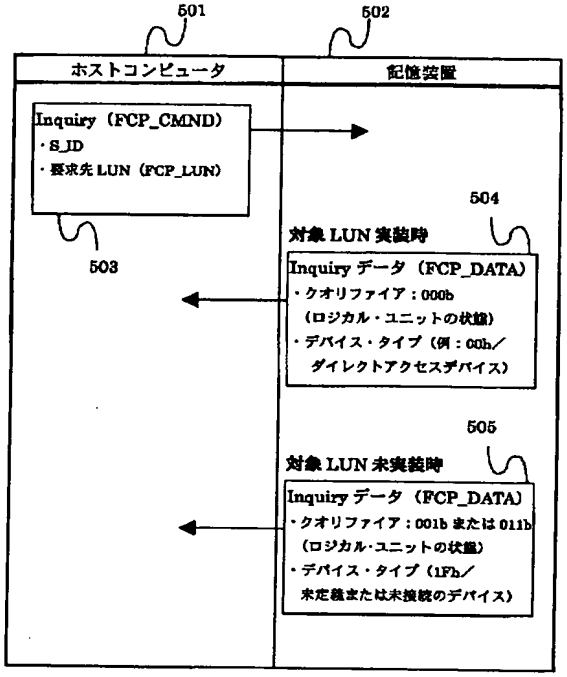
【図３】


301
302
ログイン要求元
ログイン受信先
PLOGI
・N_Port_Name
・Node_Name
・S_ID
303
304
ログイン承認時
ACC
305
ログイン拒絶時
LS_RJT

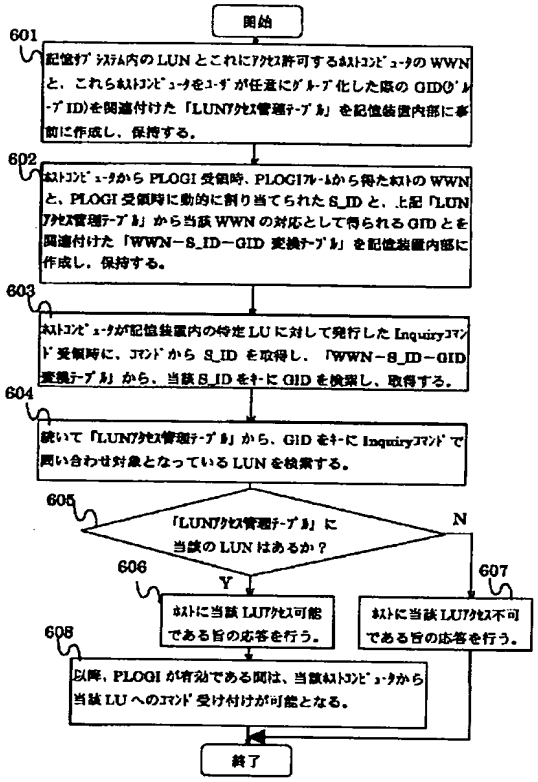
【図４】


401
402
403
SOF
フレームヘッダ
データフィールド
CRC
EOF
404
405
31-24ビット
23-16ビット
15-8ビット
7-0ビット
0 ワード
R_CTL
D_ID
1 ワード
Reserved
S_ID
2 ワード
TYPE
F_CTL
3 ワード
SEQ_ID
DF_CTL
SEQ_CNT
4 ワード
OX_ID
RX_ID
5 ワード
Parameter
406
FCP_CMND
FCP_LUN
FCP_CNTL
FCP_CDB (Inquiry)
FCP_DL
407
408
409
410

【図５】



【図６】

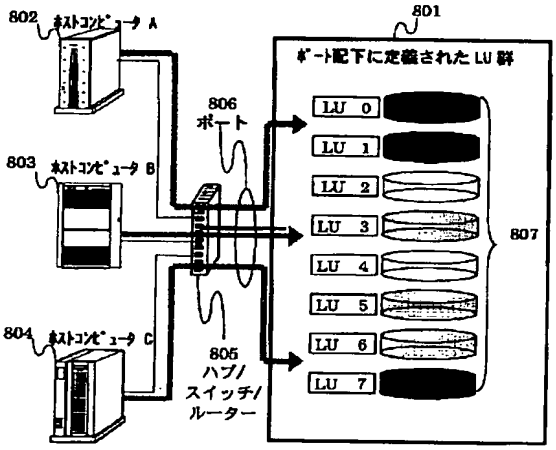


【図７】

701

	WWN	LUN
702	01234567 89ABCDEF	0 1 2
703	01234567 89ABCDEE	3 4 7
704	01234567 89ABCDED	5 6
	… … …	… … …
705	01234567 89ABCDBB	0 1 7
706	01234567 89ABCDB0	3 5 6
707	01234567 89ABCDB1	2 4

【図８】



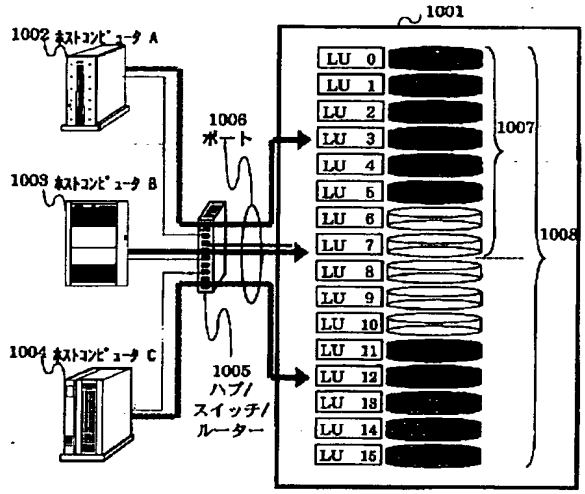
【図１６】

「WWN-S_ID-GID 変換テーブル」

1601

S_ID	WWN	G I D
FFFF01	01234567 89ABCDEF	F001
FFFF02	01234567 89ABCDEE	
FFFF03	01234567 89ABCAAC	F002
FFFF04	01234567 88ABCAA0	F002
FFFF05	01234567 88ABCBA1	F0C1
FFFF06	01234567 89ABCBBE	F01F
FFFF07	01234567 89ABCDBF	
FFFF08	01234567 89ABCDCC	F006
…	…	…

【図１０】



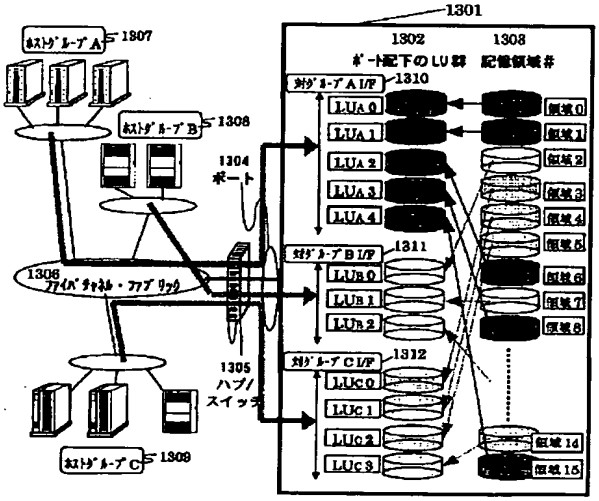
【図１１】

	GID (1102)		WWN (1103)	LUN (1104)
1105	Group A =F001 (OS 種 1)	1112	01234567 89ABCDEF	0 1 2 3
		1113	01234567 89ABCDEE	→ 記憶領域「0 1 2 3」を参照
		1114	01234567 89ABCDED	
1106	Group B =F002 (OS 種 2)	1115	01234567 89ABCDXX	0 1 2 3
		1116	01234567 89ABCDYY	→ 記憶領域
		1117	01234567 89ABCDZZ	「60 61 62 63」を参照
	... ...		... ...	... ...
1107	Group C =F003 (OS 種 3,4 混在)	1118	01234567 89AB33DD	0 1 2 3 4 5
		1119	01234567 89AB33CC	→ 記憶領域
		1120	01234567 89AB44BB	「7 11 70 79 87 119」
		1121	01234567 89AB44AA	を参照
	... ...		... ...	... ...
1108	Group D =F004 (OS 種 5,6 混在)	1122	01234567 89ABCD10	50 51 52
		1123	01234567 89ABCD2E	→ 記憶領域
				「40 99 100」を参照
	... ...		... ...	... ...
1109	Group E =F005 (OS 種 1 の 1 メンバ)	1124	01234567 89ABCD31	0 1
				→ 記憶領域「4 5」参照
	... ...		... ...	... ...
1110	Group F =F006 (OS 種 7)	1125	01234567 89ABCD46	0～2 5 5
		1126	01234567 89ABCD4E	→記憶領域「0～255」参照
1111	Group G =F007 (OS 種 7)		01234567 89ABCD46	0～2 5 5
			01234567 89ABCD4E	→記憶領域「250～512」参照
	... ...		... ...	... ...
1127	Group H =F008 (OS 種 8 Floor 1)	1129	01234567 AAABCD46	0 1
		1130	01234567 BBABCD4E	→記憶領域「10 11」参照
1128	Group I =F009 (OS 種 8 Floor 2)	1131	01234567 CCABCD46	4 5
		1132	01234567 DDABCD4E	→記憶領域「10 11」参照

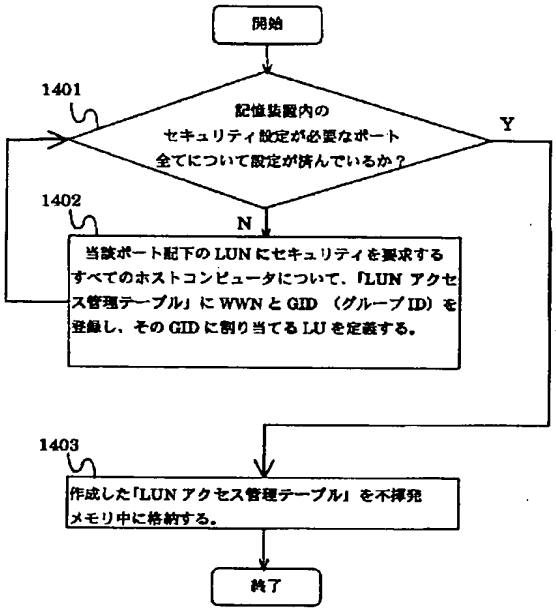
【図１２】

	GID (1202)		WWN (1201)	LUN (1203)	1204
1205	Group A (GID=F001)	1208	01234567 89ABCAAC	0 1 2 3 4	
		1209	01234567 89ABCAA0		
		1210	01234567 89ABCBA1		
1206	Group B (GID=F002)	1211	01234567 89ABCBBE	0 1 2	
		1212	01234567 89ABCDBF		
1207	Group C (GID=F003)	1213	01234567 89ABCDCC	0 1 2 3	
		1214	01234567 89ABCDC0		
		1215	01234567 89ABCDC1		
	... ...		... ...	... ...	

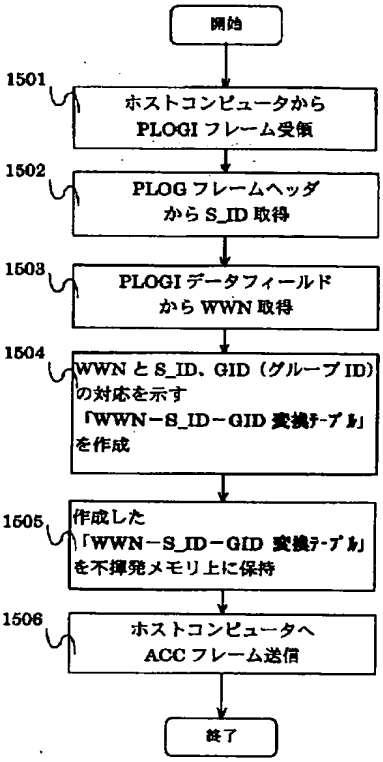
【図１３】



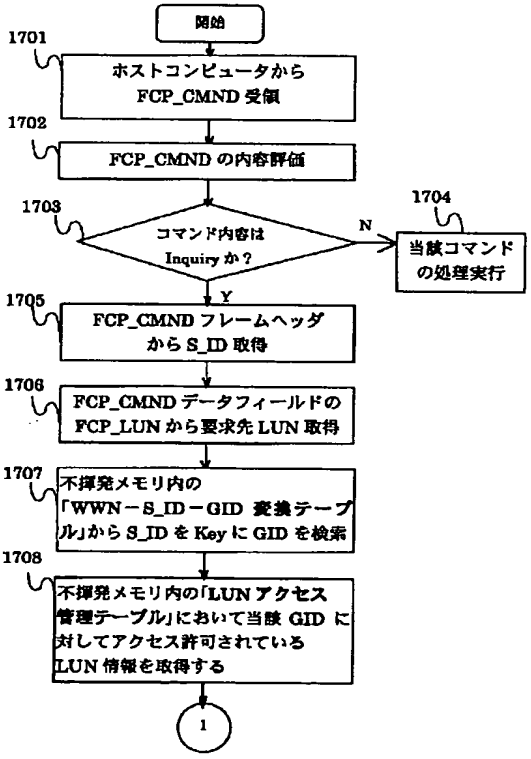
【図１４】


開始
1401
記憶装置内の
セキュリティ設定が必要なポート
全てについて設定が済んでいるか？
Y
N
1402
当該ポート配下のLUNにセキュリティを要求する
すべてのホストコンピュータについて、「LUNアクセス管理テーブル」にWWNとGID（グループID）を
登録し、そのGIDに割り当てるLUを定義する。
1403
作成した「LUNアクセス管理テーブル」を不揮発
メモリ中に格納する。
終了

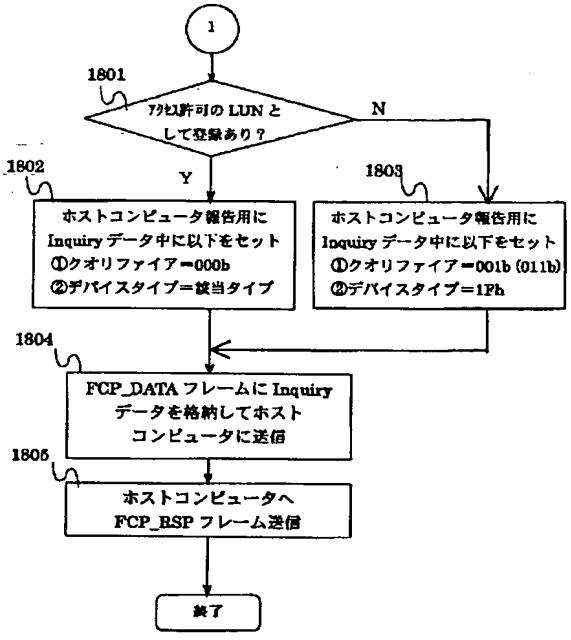
【図１５】


開始
1501
ホストコンピュータから
PLOGIフレーム受領
1502
PLOGフレームヘッダ
からS_ID取得
1503
PLOGIデータフィールド
からWWN取得
1504
WWNとS_ID、GID（グループID）
の対応を示す
「WWN－S_ID－GID変換ﾃｰﾌﾞﾙ」
を作成
1505
作成した
「WWN－S_ID－GID変換ﾃｰﾌﾞﾙ」
を不揮発メモリ上に保持
1506
ホストコンピュータへ
ACCフレーム送信
終了

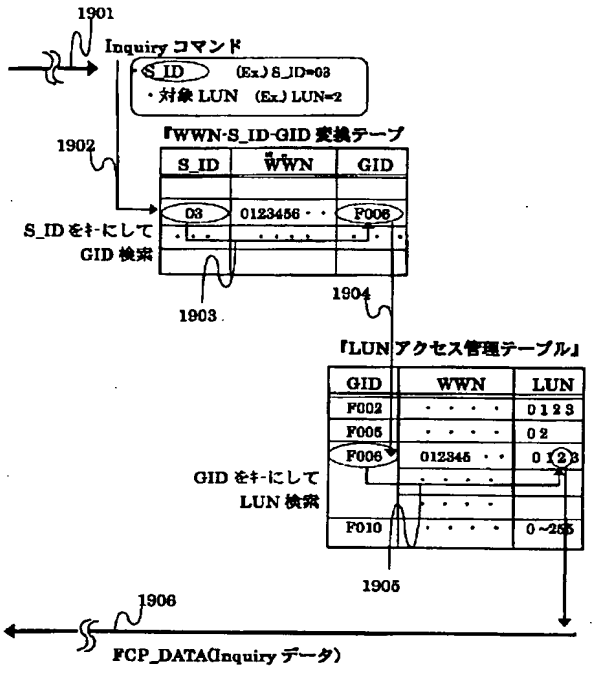
【図１７】


開始
1701
ホストコンピュータから
FCP_CMND受領
1702
FCP_CMNDの内容評価
1703
コマンド内容は
Inquiryか？
N
1704
当該コマンド
の処理実行
Y
1705
FCP_CMNDフレームヘッダ
からS_ID取得
1706
FCP_CMNDデータフィールドの
FCP_LUNから要求先LUN取得
1707
不揮発メモリ内の
「WWN－S_ID－GID変換テーブル」からS_IDをKeyにGIDを検索
1708
不揮発メモリ内の「LUNアクセス
管理テーブル」において当該GIDに
対してアクセス許可されている
LUN情報を取得する
1

【図１８】



【図１９】



フロントページの続き

(72)発明者　内海　勝広
神奈川県小田原市中里322番地２号　株式会社日立製作所ＲＡＩＤシステム事業部内
(72)発明者　五十嵐　良典
神奈川県小田原市中里322番地２号　株式会社日立製作所ＲＡＩＤシステム事業部内
(72)発明者　堀　幸一
神奈川県小田原市中里322番地２号　株式会社日立製作所ＲＡＩＤシステム事業部内

Ｆターム(参考)　5B017 AA04 BA06 BB06 CA16
5B065 BA01 CA02 CA11 PA13
5B082 EA11 JA01